*BY ORDER OF THE SECRETARY OF THE AIR FORCE*

*AIR FORCE INSTRUCTION 33-201, VOLUME 8*

*26 APRIL 2005*

*Communications and Information*

# *COMMUNICATIONS SECURITY: PROTECTED DISTRIBUTION SYSTEMS (PDS)*

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

**NOTICE:** This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ AFCA/EVPI (Mr. Gene Zuratynsky)

Certified by: HQ USAF/XICI (Lt Col Gary W. Klabunde)

Supersedes AFMAN 33-221, 12 April 2004

Pages: 44

Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*) and National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003, *Protected Distribution Systems (PDS)*. It prescribes the construction and approval requirements for a protected distribution system (PDS). This instruction applies to all Air Force military, civilian, and contractor personnel under contract by Department of Defense (DOD), who install and maintain Communications Security: Protected Distribution Systems (PDS). This instruction applies to the Air National Guard. The term major command (MAJCOM), when used in this instruction, includes field operating agencies and direct reporting units. The use of extracts from this instruction is encouraged. Additional instructions and manuals are listed on the Air Force Publishing web site at: **http://www.e-publishing.af.mil** under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this publication, through appropriate command channels, to Headquarters, Air Force Communications Agency, (HQ AFCA/EVPI), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/EASD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF IMT 847, **Recommendation For Change of Publication**. Send an information copy to HQ United States Air Force (HQ USAF/ XICI), 1800 Air Force Pentagon, Washington DC 20330-1800. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records* (will become AFMAN 33-363), and disposed of in accordance with Web-RIMS *Records Disposition Schedule (RDS)* located at: **https://webrims.amc.af.mil/rds/index.cfm**. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See **Attachment 1** for a glossary of references and supporting information.

*SUMMARY OF REVISIONS*

This change incorporates interim change (IC) 2005-1 (**Attachment 9**). It changes AFMAN 33-221 to AFI 33-201, Volume 8, to comply with Air Staff's direction to align all COMSEC publications under the AFI 33-201 umbrella. It updates office symbols, web addresses, and publications throughout the entire document. A bar ( | ) indicates a revision from the previous edition.

**1. Introduction.** AFI 33-201, (FOUO) *Communications Security (COMSEC)*, (will become AFI 33-201, Volume 1 [FOUO]), requires the use of National Security Agency (NSA)-endorsed communications security (COMSEC) products and services to secure classified telecommunications by all Air Force activities and their contractors. Information systems or networks that process classified national security information in more than one controlled-access area (CAA) and require the transfer of that information between CAAs, must use a secure means of transference-secure telecommunications or courier. If secure telecommunications is chosen, include a secure telecommunications requirement (COMSEC) in the systems security policy. In order of preference, the COMSEC requirement is met by NSA-endorsed COMSEC systems (encryption), NSA-endorsed intrusion detection optical communications system (IDOCS), or a PDS. AFI 33-201 (FOUO) (will become AFI 33-201, Volume 1 [FOUO]), also requires the use of NSA-endorsed COMSEC products, techniques, and protected services to protect certain unclassified, sensitive telecommunications involving Air Force activities and their contractors. When certain unclassified, sensitive information must be protected, and a PDS is chosen, follow the standards in this instruction for CONFIDENTIAL information. **Attachment 2** is a flow chart of the process to design, construct, approve, and operate a PDS.

1.1. Although it is less desirable than encryption, a PDS may be used to transmit unencrypted, clear-text, classified national security information. The PDS must provide adequate electrical, electromagnetic, physical, and procedural safeguards identified in this instruction. In establishing the standards for PDS construction and use, national managers incorporated the philosophy of risk management rather than risk avoidance. As such, the standards specified in this manual are the minimum protection standards based on national guidance. The assumption of any additional risk to lessen the minimum specified standards is not an option. Organizations wishing to discuss this policy may send their specific concerns through command channels to HQ AFCA/EVPI. Develop the technical solution using the process described in AFI 33-103, *Requirements Development and Processing*, to justify a PDS. Using any PDS not meeting the standards of this instruction is prohibited.

**2. Protected Distribution System Environment.** Do not use a PDS within a TEMPEST High Threat environment as defined in the Director, National Security Agency TEMPEST Threat List.

2.1. Controlled-Access Area (CAA). In this area, only personnel authorized to the level of the classified information being processed are allowed unescorted access or are under continuous physical or electronic surveillance. This area can be an office, room, group of rooms, wing, floor, or building. When the CAA is not occupied, it must be secured in such a manner such that an undetected break-in would not be possible. Within the CAA, there are three levels of control: TOP SECRET/Special Category (SPECAT), SECRET, and CONFIDENTIAL. Examples of these are open storage areas, cleared for TOP SECRET; secured facilities such as SIPRNET rooms, cleared for SECRET; and open offices that are locked at night and on weekends, cleared for CONFIDENTIAL. When two or more CAAs of the same level of control are adjoining, they can be considered one CAA and a PDS is not needed between them.

2.2. Establishing or defining both CAA boundaries is important because a PDS is installed between CAAs, usually traversing a Limited-Control Area (LCA) or an Uncontrolled Access Area (UAA). A signal line carrying classified information within the same level CAA is considered a RED signal line, although a PDS may extend into a CAA.

**3. Protected Distribution System Selection Considerations.** The "Simple" Distribution System provides a reduced level of physical protection as compared to the hardened distribution system.

3.1. Study solutions. The requesting agency, in concert with the Communications and Information Systems Officer (CSO) and Systems Telecommunications Engineering Manager (STEM), must carefully consider using a PDS before selecting it in preference to other COMSEC solutions. Economic, technical, or operational factors may make a PDS necessary in comparison to other COMSEC solutions.

3.2. Operation Considerations. Operating a PDS requires continual physical security integrity after construction. The cost and operational impact of maintaining the security of a PDS can easily exceed the construction costs. Consider using a PDS only after the requesting agency agrees to provide it the required degree of protection 24 hours-a-day, 7 days-a-week and the maintenance support required to include performing and documenting PDS line route or visual inspections as scheduled per specified intervals.

3.3. Classification Level Considerations. When reviewing communications needs, consider future requirements in regard to the classification level of the information to be transmitted, the requisite physical controls needed, and the geographical location of the PDS site. Typically it is easier and less costly to include the capability for future requirements than to retrofit an installed system for such updates.

3.4. Physical Security Considerations. The operating agency must follow normal procedures to protect the PDS terminal equipment and interconnecting signal lines within any adjoining CAA such that only persons who are cleared for the highest classification and category of information transmitted over the system may have unrestricted access to the system. Escort all personnel who do not have the appropriate security clearance, but require occasional, temporary access to the PDS terminal equipment and interconnecting lines (e.g., safety and fire inspectors) to prevent a compromise of the information or the security integrity of the PDS. Maintain the physical security integrity of the PDS on a continual basis, regardless of whether the PDS is in continuous operation or not. The intent is to detect any signs of tampering or penetration as early as possible, and before the system is used again.

3.5. Signal wires in PDS. Do not run BLACK signal wire lines in a PDS with RED signal wire lines because of crosstalk. BLACK fiber optic signal lines may be run in a PDS with RED signal lines, but is discouraged for three reasons. It is difficult to identify BLACK signal lines anywhere within the PDS except at the ends. Any person with a need to access the BLACK signal lines must have the appropriate clearance or be escorted. All breakouts of BLACK signal lines must be made in a CAA. See AFMAN 33-214, Volume 2, *Emission Security Countermeasures Review* (will become AFI 33-203, Volume 3).

**4. Protected Distribution System Justification.** Justify a PDS using the technical solution process of AFI 33-103 and meet the requirements of this manual before approving construction or use. The requesting agency, CSO, and STEM must justify using a PDS instead of an approved COMSEC system, IDOCS, or courier before submitting the technical solution for approval.

4.1. Justify the PDS by:

4.1.1. Showing that courier is not timely, practical, or feasible.

4.1.2. Using a capability or cost basis.

4.2. If the justification is based on capability, the CSO must show:

4.2.1. There is no COMSEC system or IDOCS with the capability to handle the data to be passed over the PDS.

4.2.2. A capable COMSEC system exists; however, equipment is not available to support this requirement. IDOCS provides the capability to secure communications over optical fiber lines without the use of encryption or a PDS.

4.3. If the justification is based on cost, the requesting agency must clearly indicate a PDS is less costly than using an approved COMSEC system or IDOCS. When this justification is used, compare and show the total life-cycle cost of COMSEC equipment or IDOCS to the total life-cycle cost of the proposed PDS. As a minimum, the PDS plan must show the following:

4.3.1. PDS construction costs.

4.3.2. Annual operation and maintenance costs.

4.3.3. Annual physical security costs.

4.4. The justification is the first document of the PDS package file (see **Figure 1.**). A separate file is required for each PDS.

**Figure 1. The PDS Package File.**


**5. Protected Distribution System (PDS) Plan.** The requesting agency must prepare a PDS plan prior to constructing a PDS. Obtain a PDS identification number from the wing Information Assurance (IA) office. This number consists of the MAJCOM, the base, and a unique three-digit number (e.g., AMC-Scott-001). This plan identifies and assigns responsibility for operational security requirements and specifies the design and construction requirements.

5.1. Information and Access Requirements. Identify:

5.1.1. Highest classification level and category of information carried by the PDS.

5.1.2. Minimum-security clearance level of individuals with unrestricted access to any portion of the PDS.

5.2. User Information. Identify:

5.2.1. Name and location of the requesting agency. This will normally be the office of record for the PDS. The office of record will maintain the PDS file.

5.2.2. Name, organization, and office symbol of the Designated Approving Authority (DAA) (see paragraph **9.**).

5.2.3. CAAs (buildings and room numbers) connected by the PDS. There are three levels of control for CAAs: open storage areas, secured facilities, and open offices that are locked at night and on weekends (see definition of CAA). The open offices present the most difficulties in meeting security requirements.

5.2.4. Organizations and office symbols occupying the CAAs identified in paragraph **5.2.3.** connected by the PDS.

5.3. PDS Operation Requirements. Specify the operation requirements (see **Attachment 3**). Document each requirement with an official memorandum, a letter of appointment, an operating instruction, or other official means. Drafts are permitted for validation. Finalize drafts prior to certification.

5.3.1. Identify type of PDS chosen, Hardened or Simple:

5.3.1.1. If Hardened PDS, identify type of Hardened PDS chosen:

5.3.1.2. Above ground or buried;

5.3.1.3. Alarmed or not alarmed; or

5.3.1.4. Continuously viewed.

5.3.2. PDS Physical Security Requirements. Identify the physical security requirements from **Attachment 4**.

5.3.3. PDS Signal Line Requirements. Identify the signal line requirements from **Attachment 5**.

5.3.4. PDS Construction Requirements. Identify the physical construction requirements from **Attachment 6**. Identify the organization proposed to install the PDS.

5.3.5. Circuit Separation Requirements. Refer to **Attachment 7** for circuit separation criteria when sharing a single distribution system.

**6. Protected Distribution System (PDS) Plan Validation.** The requesting agency submits a copy of the PDS justification and the PDS plan to the wing IA office for validation.

6.1. The wing IA office reviews the justification for adequacy and the plan for obvious errors such as requiring unnecessary redundancy in protection or any major omissions. If all the operational security requirements are met, the wing IA office validates the PDS plan and creates a PDS file (see **Figure 1.**).

6.2. Document the validation as a memorandum. Attach the validation to the PDS file (see **Figure 1.**).

6.3. The wing IA office keeps the copy of the PDS file to be used during certification.

6.4. Modifications. When proposing a modification to an existing PDS, the wing IA office, in coordination with the requesting agency, determines the need for a new or revised PDS plan based on the increased size and complexity of the existing PDS itself. The wing IA office may request a cost analysis to ensure that a PDS is still the best solution.

**7. Protected Distribution System (PDS) Construction.** Construct the PDS according to the validated plan. Do not use the PDS to pass classified national security information until the PDS is approved by the DAA. Document all deviations. Deviations are defined as minor changes made during the installation, such as different routing of conduit, discontinuance of a feeder line or even the addition of a high-priority user on the PDS while the system is being installed and after the plan is approved. All members of the team constructing the PDS must have an appropriate security clearance to prevent any instance of "pre-tampering" of the system. If adequately cleared personnel are not available, uncleared installers or construction workers must be escorted at all times by someone from outside the team with an appropriate clearance. The escort must have sufficient technical knowledge to recognize any attempts of tampering or penetration.

**8. Protected Distribution System (PDS) Certification.** After construction and installation, and prior to using the PDS, the requesting agency requests certification from the wing IA office. Provide the wing IA office documentation for any deviations from the plan. The deviation documentation becomes a part of and is attached to the original PDS plan. Include finalized instructions, memorandums, and letters of agreement. Replace the drafts with the final documents in the PDS file. The wing IA office reviews the plan and the deviations.

8.1. The wing IA office certifies:

8.1.1. Compliance with the construction plan, including deviations.

8.1.2. Successful completion of prescribed lines route inspection, as required.

8.1.3. Alarm circuit verification procedures, as required.

8.1.4. Continuous viewing procedures, as required.

8.1.5. The PDS passed a technical inspection by the technical inspector, (usually designated by the wing IA office [see **Attachment 8**.]).

8.1.6. The controlling office is identified.

8.1.7. The incident reporting and investigating system is in effect.

8.2. The wing IA office:

8.2.1. Ensures all discrepancies are corrected before certifying the PDS.

8.2.2. Documents the certification as a memorandum. Attaches the certification memorandum to the PDS file (see **Figure 1.**).

8.2.3. Keeps a copy and sends the certification to the requesting agency.

8.2.4. Attaches any deviations and the certification to the PDS file (see **Figure 1.**).

**9. Protected Distribution System (PDS) Approval.**

9.1. Approving the PDS. The requesting agency submits the PDS certification memorandum to the DAA. The DAA approves operation of the PDS as part of the System Security Authorization Agreement (SSAA) (formerly certification and accreditation [C&A]). The PDS file is separate from the SSAA.

9.2. Filing the Approval. Send a copy of the approval to the wing IA office for their files. The wing IA office attaches the PDS approval to the PDS file as shown in **Figure 1.**

9.3. Approving Authorities. Except as noted below, the DAA approves the PDS as a part of the SSAA process for the network or information system the PDS is supporting. AFPD 33-2 requires that all systems be certified and accredited prior to operation. AFI 33-202, *Networks and Computer Security*, (will become AFI 33-202, Volume 4, *Certification and Accreditation),* details the process used to certify and accredit Air Force systems. Complete the requirements of AFI 33-202, (will become AFI 33-202, Volume 4), before obtaining approval to operate.

9.3.1. Temporary Systems. The DAA may approve temporary system configurations without processing a formal approval package after meeting all the following conditions:

9.3.1.1. The PDS is in place no more than 1 month.

9.3.1.2. The PDS is confined within U.S. Government installations.

9.3.1.3. The PDS will not process higher than SECRET information.

9.3.2. Contractor Facilities. The head of the government contracting department or agency is the approving authority for a contractor-owned and operated PDS.

9.3.3. Tactical Systems. Mobile systems employing inter-shelter PDS need not be re-approved for each relocation if the relocation provides security comparable to that of the original approval, as determined by the local IA office. Otherwise, new approval must be obtained.

9.3.4. Systems without a DAA. For those systems not requiring a DAA, the approving authority is the unit commander.

**10. Protected Distribution System (PDS) Recertification.**

10.1. The wing IA office recertifies a PDS as part of the system recertification and reaccreditation:

10.1.1. Every 3 years, if installed within the United States, its trust territories, and possessions (hereafter called the U.S.).

10.1.2. Annually, if installed outside the U.S.

10.2. Recertify the PDS after verifying the following:

10.2.1. Lines route inspections (if needed): The PDS meets requirements and previous inspections were completed on schedule.

10.2.2. Technical inspections: The PDS was within limits and the inspections were completed on schedule (see **Attachment 8**).

10.2.3. Alarm circuit (if used) verification: Previous alarm circuit tests were successful and completed on schedule.

10.2.4. PDS events record: Evidence that this record is current and includes all significant events.

10.3. Attach the recertification to the PDS file as shown in **Figure 1.**

10.4. A PDS that does not meet the above requirements may not be recertified.

10.4.1. The wing IA office notifies the DAA immediately when a PDS is not recertified.

10.4.2. The PDS is shut down immediately.

10.4.3. The requesting agency corrects deficiencies discovered during recertification within 30 days and requests recertification. The Certified TEMPEST Technical Authority (CTTA) may be consulted for clarification on site-specific PDS items.

10.4.4. A PDS that fails recertification cannot be used until recertified.

**11. Protected Distribution System (PDS) Deactivation.** The operating agency reports deactivation of an approved PDS to the DAA and wing IA office within 5 days of deactivation. The Master PDS Plan and files pertaining to the deactivated PDS shall be marked "DEACTIVATED ON (Date)"

**12. Information Collections, Records, Forms or Information Management Tools (IMT)** .

12.1. Information Collections. No information collections are created by this publication.

12.2. Records. Maintain and dispose of program records created by this publication accordance to Air Force Web-RIMS (RDS), Table 33-22 and Rule 13, located at: **https://webrims.amc.af.mil/rds/index.cfm**.

12.3. Forms or IMTs.

12.3.1. Adopted Forms or IMTs. AF Form 847, **Recommendation for Change of Publication**.

12.3.2. Prescribed Forms or IMTs. No forms are prescribed by this publication.

WILLIAM T. HOBBINS, Lt General, USAF
DCS, Warfighting Integration

**Attachment 1**

**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION**

***References***

DOD 5200.1-R, *Information Security Program*, January 1997

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFI 31-101, (FOUO) *The Air Force Installation Security Program*

AFI 33-103, *Requirements Development and Processing*

AFI 33-201, (FOUO) *Communications Security (COMSEC)*
(will become AFI 33-201, Volume 1 [FOUO])

AFI 33-202, *Network and Computer Security* (will become AFI 33-202, Volume 4, *Certification and Accreditation)*

AFI 33-212, *Reporting COMSEC Deviations* (will become AFI 33-201, Volume 3 [FOUO])

AFMAN 33-214, Volume 1, (S) *Emission Security Assessments* (U)
(will become AFI 33-203, Volume 2 [S])

AFMAN 33-214, Volume 2, *Emission Security Countermeasures Reviews*
(will become AFI 33-203, Volume 3)

AFMAN 37-123, *Management of Records* (will become AFMAN 33-363)

AFDIR 33-303, *Compendium of Communications and Information Terminology*

NSTISSI No. 7003, *Protected Distribution Systems (PDS)*

Web-RIMS, *Records Disposition Schedule (RDS)*

***Abbreviations and Acronyms***

**AFCA—**Air Force Communications Agency

**AFDIR—**Air Force Directory

**AFI—**Air Force Instruction

**AFMAN—**Air Force Office of Special Investigation

**AFPD—**Air Force Policy Directive

**C&A—**Certification and Accreditation

**CAA—**Controlled Access Area

**COMSEC—**Communications Security

**CSO—**Communications and Information Systems Officer

**CTTA—**Certified TEMPEST Technical Authority

**DAA—**Designated Approving Authority

**dB—**Decibels

**DOD—**Department of Defense

**EMSEC—**Emission Security

**EMT—**Electrical Metallic Tubing

**FOUO—**For Official Use Only

**GFSP—**General Field Service Padlock

**GSA—**General Services Administration

**IA—**Information Assurance

**IDOCS—**Intrusion Detection Optical Communications System

**LCA—**Limited Controlled Area

**MAJCOM—**Major Command

**MHz—**Megahertz

**NSA—**National Security Agency

**NSN—**National Stock Number

**NSTISSI—**National Security Telecommunications and Information Systems Security Instruction

**PDS—**Protected Distribution System

**SIPRNET—**Secret Internet Protocol Router Network

**SSAA—**System Security Authorization Agreement

**SPECAT—**Special Category

**STEM—**Systems Telecommunications Engineering Manager

**STP—**Shielded Twisted-Pair

**TDR—**Time Domain Reflectometry

**UAA—**Uncontrolled Access Area

**USAF—**United States Air Force

**WWW—**World Wide Web

***Terms***

**Access Control—**Process of limiting access to the resources of an information system only to authorized users, programs, processes, or other systems.

**Controlled-Access Area (CAA)—**The room, building, or facility area under direct physical control within which unauthorized persons are denied unrestricted access and are either escorted by authorized persons or are under continuous physical or electronic surveillance. Within the greater CAA, there are three levels of data control: TOP SECRET/SPECAT, SECRET, and CONFIDENTIAL. Examples of these are open storage areas, secured facilities, and open offices that are locked at night and on weekends. These levels correspond to division of **Table A4.1.** and **Table A4.2.**

**Limited-Control Area (LCA)—**The space surrounding a protected distribution system within which exploitation is not considered likely or legal authority to identify or remove a potential exploitation exists. Also known as Inspectable Space.

**Line Route—**The actual path of the PDS, including the conductor, inside the PDS.

**Lockbox—**A metallic box with a lock attached to the end of the PDS within the CAA large enough to hold the signal line. The purpose of the lockbox is to provide authorized access to classified information when, and only when, required. Normally, the lockbox houses a live Secret Internet Protocol Router Network (SIPRNET) connection point and therefore is a security container. The lockbox can use an approved padlock or the newer lockbox can use a high security combination lock or electronic lock, similar to the lock on a safe. Lockboxes should be General Service Administration (GSA) approved containers; are covered under DoD 5200.1-R, *Information Security Program*, January 1997; and require a SF 702. See paragraph **A6.4.1.7.** for more information.

**Protected Distribution System (PDS)—**A wire line or fiber optics distribution system with adequate electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified national security information. ***NOTE***: This definition does not include IDOCS approved by the NSA.

**Special Category (SPECAT)—**The definition is classified (see AFMAN 33-214, Volume 1 [S] *Emission Security Assessment* [U], (will become AFI 33-203, Volume 2 [S]).

**Uncontrolled Access Area (UAA)—**The area external or internal to a facility over which no personnel access controls can be or are exercised. The area outside the fence surrounding an Air Force Base, and accessible to the general public is an UAA.

**Table A1.1. World Wide Web (WWW) Sources.**

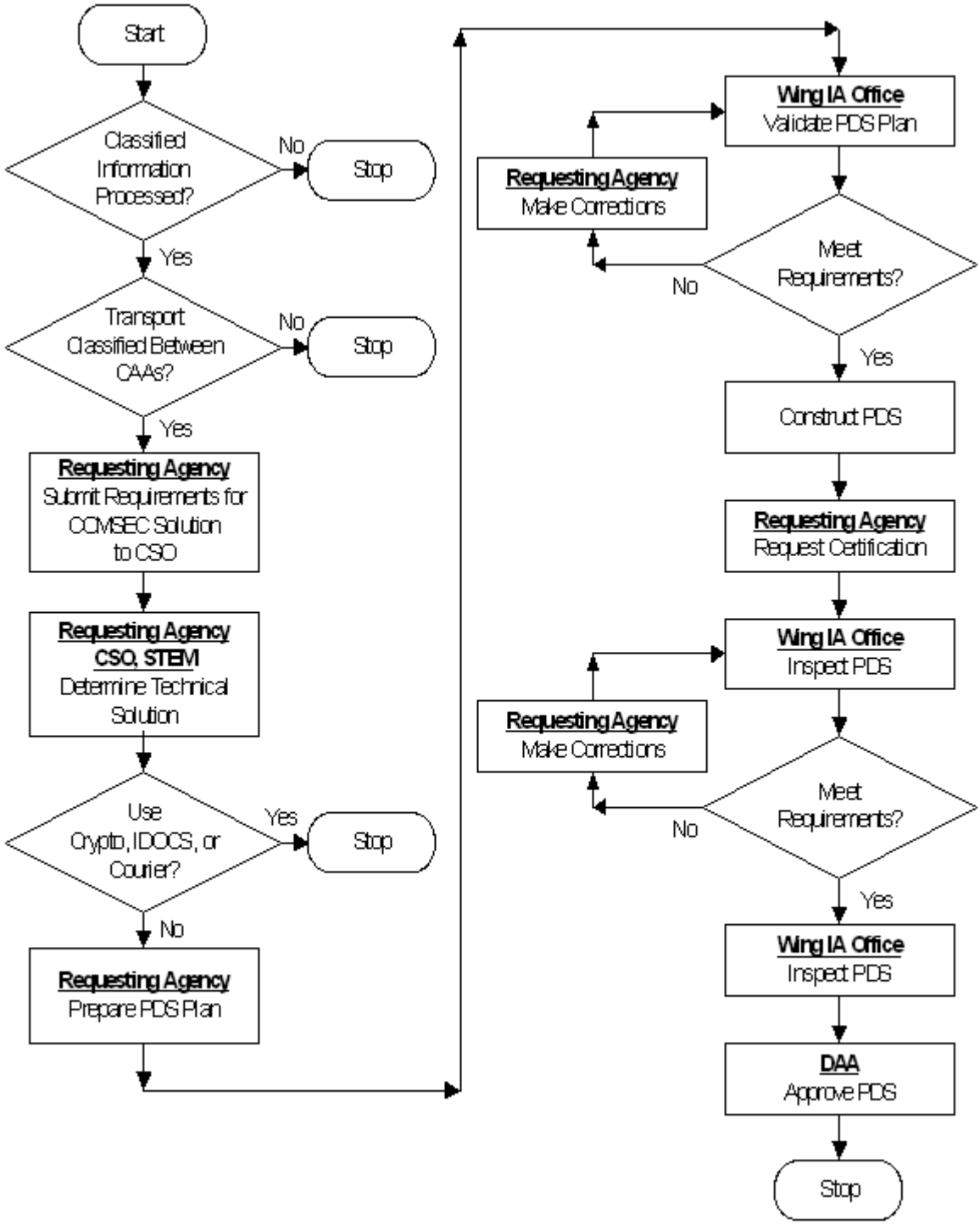
| Referenced | URL | Topic | Organization | Web Page POC |
|---|---|---|---|---|
| **Attachment 1** | **https://private.afca.af.mil/ip/** | Information Assurance web page | HQ AFCA/ EVPI | Web Master: **EVPI Webmaster@scott.af.mil** |
| Purpose Statement | **http://www.e-publishing.af.mil** | Air Force Publishing | AFDPO | **e-publishing@pentagon.af.mil** |
| Purpose Statement | **https://webrims.amc.af.mil/rds/index.cfm** | Web-RIMS RDS | AFCA/RIMS | **web.records@scott.af.mil** |

## Attachment 2

## PROTECTED DISTRIBUTION SYSTEMS (PDS) PROCESS FLOW CHART

**A2.1.** **Figure A2.1.** is a flow chart of the process to design, construct, and approve a PDS.

**Figure A2.1. The PDS Plan, Validation, Construction, Certification, and Approval Process.**



## Attachment 3

## PROTECTED DISTRIBUTION SYSTEMS (PDS) OPERATION REQUIREMENTS

**A3.1. Introduction.** This attachment identifies the operation requirements needed to ensure and maintain the security of the PDS. The operation requirements listed in this attachment are the minimum requirements. Document these requirements with an official memorandum, such as a letter of appointment, an operating instruction, or other official means. Ensure that the wing IA office is kept aware of new PDSs or modifications to existing PDSs. Advise the local Staff Judge Advocate when the PDS traverses UAAs.

**A3.2. Controlling Office.** The Controlling Office is the office of primary responsibility for the PDS operation; with the IA office, civil engineer, and the DAA playing major roles. The DAA is the final authority granting approval to operate.

A3.2.1. Establish the operational security procedures for the PDS. Draft procedures are permitted for validation (see paragraph **6.**). Finalize them for certification (see paragraph **8.**).

A3.2.2. Establish the requirement for all personnel in the CAAs to be aware of their responsibility to assist in the close supervision of the visible components of the PDS. They are to report all incidents of suspicious activity immediately.

**A3.3. Security Office.** Identify a PDS security office or person (may be the same as the Controlling Office or the Record Office). Neither the MAJCOM nor the wing IA office will be identified as the Security Office. This office or person will:

A3.3.1. Establish and review the PDS .Log at least monthly.

A3.3.2. Receive reports of alarms (if used) and incidents of tampering, penetration, or unauthorized interception, immediately make the initial investigation, and resolve or notify the specified investigating agency such as Security Forces, Air Force Office of Special Investigations (AFOSI), etc.

A3.3.3. Receive reports of suspicious activity in the area of the PDS, immediately make the initial investigation, and resolve or report such activities to security forces for appropriate action.

A3.3.4. Make required notifications.

**A3.4. Record Office.** Specify the office, or person, to establish and maintain a record of events for the PDS (may be the same as the Controlling Office or the Security Office). Neither the MAJCOM nor the wing IA office will be identified as the Record Office. Record in the PDS Log, all PDS events such as alarms, lines route inspections, technical inspections, and other pertinent information.

**A3.5. Reporting Procedures.** Establish the procedures for reporting incidents of tampering, penetration, or unauthorized interception. These incidents will most likely be discovered during lines route inspections and technical inspections. Ensure these incidents are reported immediately. Specify the means for reporting such as secure telephone, in person, etc. Include the requirement to immediately discontinue using the PDS until the approval authority assesses the incident and its security status is determined.

A3.5.1. Immediately report these incidents to the PDS Security Office, or person, for review and initiation of an investigation.

A3.5.2. Immediately report these incidents as a physical security COMSEC incident following the procedures established for physical security incidents in AFI 33-212, *Reporting COMSEC Deviations* (will become AFI 33-201, Volume 3 [FOUO])

**A3.6. Investigating Procedures.** Establish the procedures for investigating reports of tampering, penetration, or unauthorized interception. This should involve the AFOSI since these incidents could be acts of espionage.

**A3.7. Monitoring Alarms.** If the PDS is alarmed, identify who will monitor the alarm indicator.

**A3.8. Responding to Alarms.** If the PDS is alarmed, establish the requirement to respond to an alarm within 15 minutes and identify the individuals responding.

**A3.9. Investigating Alarms.** If the PDS is alarmed, identify who will initially investigate alarms to determine if an attempt at tampering, penetration, or unauthorized interception is suspected. If an attempt is suspected, notify the specified investigating agency; typically, this is the AFOSI.

**A3.10. Inspections.** Specify the office that will be responsible for conducting the required inspections as delineated in **Attachment 4**.

**A3.11. Testing Requirements.** Each alarm system is unique and therefore has unique testing requirements. Refer to the Vendor's operating and testing instructions.

## Attachment 4

## PROTECTED DISTRIBUTION SYSTEMS (PDS) PHYSICAL SECURITY REQUIREMENTS

**A4.1. General.** This attachment provides requirements for selecting the appropriate type of distribution system to provide the required physical security for the signal line. The intent of operational security procedures in combination with construction requirements allows for rapid detection of any attempted penetration of the PDS rather than ensuring the prevention of a penetration. Varying degrees of protection are based on the PDS construction and other physical protection measures incorporated.

**A4.2. Determine Type of Distribution System.** Identify the highest security classification of information, including SPECAT, using the system and the type of area to be traversed by the PDS (UAA, LCA, or CAA). Use **Table A4.1.** and **Table A4.2.** to determine the type of distribution system required, simple or hardened. Note that the threat level associated with a base is classified CONFIDENTIAL. If the PDS plan states either the threat level or which table was used, this information is classified CONFIDENTIAL.

**Table A4.1. Required Type of Distribution Systems within the U.S. and Outside the U.S. Low Threat.**

| | | Type of Area TRAVERSED | | | | |
|---|---|---|---|---|---|---|
| | **TYPE OF DATA** | **UAA** | **LCA** | **CONFIDENTIAL CAA** | **SECRET CAA** | **TOP SECRET CAA** |
| **1** | **CONFIDENTIAL** | Hardened | Simple | (NOTE) | (NOTE) | (NOTE) |
| **2** | **SECRET** | Hardened | Hardened | Simple | (NOTE) | (NOTE) |
| **3** | **TOP SECRET** | Hardened | Hardened | Simple | Simple | (NOTE) |
| **4** | **SPECAT** | Hardened | Hardened | Simple | Simple | Simple |
| ***NOTE:*** PDS not required, consider as a RED signal line within the CAA. | | | | | | |

**Table A4.2. Required Type of Distribution Systems Outside the U.S. – Medium Threat.**

| | | Type of Area TRAVERSED | | | | |
|---|---|---|---|---|---|---|
| | **TYPE OF DATA** | **UAA** | **LCA** | **CONFIDENTIAL CAA** | **SECRET CAA** | **TOP SECRET CAA** |
| **1** | **CONFIDENTIAL** | Hardened | Simple | (NOTE) | (NOTE) | (NOTE) |
| **2** | **SECRET** | Hardened | Hardened | Simple | (NOTE) | (NOTE) |
| **3** | **TOP SECRET** | Hardened | Hardened | Hardened | Simple | (NOTE) |
| **4** | **SPECAT** | Hardened | Hardened | Hardened | Simple | Simple |
| ***NOTE:*** PDS not required, consider as a RED signal line within the CAA. | | | | | | |

**A4.3. Hardened Distribution System.** Identify the type of hardened carrier (above ground or buried, alarmed or continuously viewed) to be used.

A4.3.1. Hardened Carrier: If a hardened carrier was chosen.

A4.3.1.1. All security requirements must be enforced 24 hours-a-day, 7 days-a-week, whether or not the PDS is in continuous operation.

A4.3.1.2. Do not conceal a hardened carrier from view behind walls, above ceilings, or below floors, unless it is alarmed. If the carrier is even partially concealed from view, it must be alarmed. In lieu of alarming the carrier, and within the U.S., the carrier may be buried a minimum of 1 meter deep. If buried on an installation outside the U.S., in a MEDIUM or higher threat location, the carrier must be encased in concrete and buried a minimum of 1 meter deep. The concrete encasement must be a minimum of 20 centimeters (8 in.) in all directions.

A4.3.1.3. Secure the termination when the network security policy requires it. Normally, the termination is secured when not in use and the signal lines from the carrier terminate at a user equipment terminal location not maintained as a CAA 24 hours-a-day, 7 days-a-week. This requirement usually does not apply to CAAs accredited for open storage or CAAs in secure facilities (e.g., a Sensitive Compartmented Information Facility {SCIF}). Solutions are: (1) Shut down the circuit to the unattended terminal; (2) Use a lockbox.

A4.3.1.4. Lines route visual inspection requirements.

A4.3.1.4.1. Identify the required minimum interval for lines route visual inspections from **Table A4.3.** (this information, when applied to a specific PDS, is CONFIDENTIAL). Daily inspections must be performed on weekends and holidays, as specified.

A4.3.1.4.2. A line route inspection consists of a close visual inspection of the PDS for signs of penetration, tampering, and any other anomaly that may cause a deterioration of protection safeguards. The close visual inspection must include the total surface (360 degrees) of the PDS (especially those parts close to walls); use of a mirror is recommended. For buried PDS, the visual inspection must extend 5 meters (16 feet) on either side of the PDS route; inspect for evidence of unauthorized digging.

A4.3.1.4.3. PDS lines route inspectors need not be qualified installers or technicians, but must recognize physical changes in the PDS including attempts at penetration or tampering.

**Table A4.3. PDS Lines Route Visual Inspection Schedule. (NOTE 1)**

| | HIGHEST CLASSIFICATION OF DATA CARRIED | Facility Location | | | | | |
|---|---|---|---|---|---|---|---|
| | | WITHIN THE U.S. | | OUTSIDE THE U.S. LOW THREAT (NOTE 2) | | OUTSIDE THE U.S. MEDIUM THREAT (NOTE 2) | |
| | | UAA | LCA | UAA | LCA | UAA | LCA |
| 1 | SPECAT or Top Secret | 2 | 1 | 2 | 1 | 6 | 3 |
| 2 | Secret | 1 | 1(NOTE 3) | 1 | 1(NOTE 3) | 4 | 2 |
| 3 | Confidential | 1 | None | 1 | None | 2 | 1 |

***NOTES:***

1. Minimum number of randomly scheduled inspections per day per location.
2. The TEMPEST threat environment is defined by NSA.
3. For buildings that are secured when not occupied (nights and weekends); lines route inspections may be accomplished on a weekly basis.

A4.3.1.5. Technical inspection requirements.

A4.3.1.5.1. Identify the minimum interval to perform technical inspections from **Table A4.4.** (this information, when applied to a specific PDS, is CONFIDENTIAL). Note that the threat level associated with a base is classified CONFIDENTIAL. If the PDS plan states either the threat level or which table was used, this information is classified CONFIDENTIAL.

A4.3.1.5.2. Specify the office or organization responsible for performing the technical inspections. Technical inspection requirements are defined in **Attachment 8**.

**Table A4.4. PDS Technical Inspection Schedule. (NOTE 1)**

| HIGHEST CLASSIFICATION OF DATA CARRIED | | FACILITY LOCATION | | |
|---|---|---|---|---|
| | | WITHIN THE U.S. | OUTSIDE THE U.S. LOW THREAT (NOTE 2) | OUTSIDE THE U.S. MEDIUM THREAT (NOTE 2) |
| 1 | SPECAT or Top Secret | 1 | 1 | 4 |
| 2 | Secret | 1 | 1 | 2 |
| 3 | Confidential | 1 | 1 | 1 |

***NOTES:***

1. Minimum number of randomly scheduled technical inspections per year.
2. The threat environment is defined by NSTISSI 7000, (C) *TEMPEST Countermeasures for Facilities* (U), Annex A, (S) *TEMPEST Threat to Facilities* (U) or the NSA TEMPEST Threat List.

A4.3.2. Alarmed Carrier.

A4.3.2.1. All security requirements must be enforced 24 hours-a-day, 7 days-a-week whether or not the PDS is in continuous operation.

A4.3.2.2. Identify the office to monitor the PDS alarm, 24 hours-a-day, 7 days-a-week.

A4.3.2.3. Specify the required responses to alarm conditions (this information, when applied to a specific PDS, is For Official Use Only [FOUO]).

A4.3.2.4. Identify the office that will respond to PDS alarms.

A4.3.2.5. Establish the required minimum interval for alarm circuit verification from **Table A4.5.** (this information, when applied to a specific PDS, is FOUO).

**Table A4.5. Alarm Circuit Verification Schedule.**

| HIGHEST CLASSIFICATION OF DATA CARRIED | | INTERVAL |
|---|---|---|
| 1 | SPECAT or TOP SECRET | Monthly |
| 2 | Secret | Quarterly |
| 3 | Confidential/UNCLASSIFIED SENSITIVE | Quarterly |

A4.3.2.6. Technical inspection requirements.

A4.3.2.6.1. Identify the minimum interval to make technical inspections from **Table A4.4.** (this information, when applied to a specific PDS, is CONFIDENTIAL).

A4.3.2.6.2. Specify the office or organization responsible for conducting the technical inspections. Technical inspection requirements are defined in **Attachment 8**.

A4.3.2.7. Alarmed carriers do not require lines route inspections.

A4.3.3. Continuously Viewed Carrier.

A4.3.3.1. All security requirements must be enforced 24 hours-a-day, 7 days-a-week whether or not the PDS is in continuous operation.

A4.3.3.2. Identify the office to provide the monitoring service.

A4.3.3.3. A continuously viewed carrier must be under continual observation (24-hours-a-day, 7 days-a-week), whether in use or not.

A4.3.3.4. Technical inspection requirements.

A4.3.3.4.1. Identify the required minimum interval to make the technical inspections from **Table A4.4.** (this information, when applied to a specific PDS, is CONFIDENTIAL).

A4.3.3.4.2. Specify the office or organization responsible for conducting the technical inspections. Technical inspection requirements are defined in **Attachment 8**.

A4.3.3.5. Continuously viewed carriers do not require lines route inspections.

**A4.4. Simple Distribution System.** This system provides a reduced level of physical protection as compared to the hardened distribution system.

A4.4.1. All security requirements must be enforced 24 hours-a-day, 7 days-a-week, whether or not the PDS is in continuous operation.

A4.4.2. When designing and installing a simple carrier, it may be installed behind walls, above ceilings, or below floors, as long as it can be inspected. A concealed simple carrier must be installed within a LCA or CAA. See **Table A4.1.** and **Table A4.2.** for maximum level of data classification.

A4.4.2.1. See paragraph **A4.4.4.** for lines route inspection requirements and paragraph **A4.4.5.** for technical inspection requirements.

A4.4.3. Secure the termination when the network security policy requires it. Normally, you are required to secure the termination when the termination is not in use and the signal lines from the carrier terminate at a user equipment terminal location not maintained as a CAA 24 hours-a-day, 7 days-a-week.

This requirement usually does not apply to CAAs accredited for open storage or CAAs in secure facilities (e.g., a SCIF).

A4.4.4. Identify the lines route inspection requirements.

A4.4.4.1. Identify the required minimum interval for lines route inspections. For simple PDS in LCAs, conduct lines route inspection monthly. For simple PDS in CAAs, conduct lines route inspection quarterly (this information, when applied to a specific PDS, is FOUO).

A4.4.4.2. Specify the office that will make the lines route inspections.

A4.4.4.3. A lines route inspection consists of a close visual inspection of the carrier for signs of penetration, tampering, and any other anomaly that may cause a deterioration of protection safeguards; use of a mirror is recommended.

A4.4.4.4. The persons selected to accomplish the lines route inspections need not be qualified installers or technicians, but they must know enough about the carrier construction to recognize physical changes in the carrier including attempts at penetration and tampering.

A4.4.5. Identify the technical inspection requirements.

A4.4.5.1. Identify the required minimum interval to make the technical inspections from **Table A4.4.** (this information, when applied to a specific PDS, is FOUO).

A4.4.5.2. Specify the office or organization that will make the technical inspections or ensure inspections are completed. Technical inspection requirements are defined in **Attachment 7**.

A4.4.5.3. In buildings that are secured when not occupied and the simple carrier is concealed, you must make a technical inspection whenever there is evidence of a forced or unauthorized entry to the secured building.

**A4.5. Tactical Arena.**

A4.5.1. In tactical environments, locate the PDS within areas directly under U.S. Forces physical control.

A4.5.2. Protect the perimeters of the PDS. Keep under surveillance with armed guards or patrols.

A4.5.3. Provide protection commensurate with the level of information passed through the PDS.

A4.5.4. The responsible commander assesses the risks associated with maintaining the security of the system. Include factors such as stability of the area and technical intelligence collection proficiency of adversaries, to include the host country, and their capability to collect and relay information obtained.

**A4.6. Marking a Protected Distribution System (PDS).** Do not mark a PDS outside the CAA. The COMSEC requirement to mark all RED signal lines with red tape or paint applies only to RED signal lines within the CAA.

## Attachment 5

## PROTECTED DISTRIBUTION SYSTEM (PDS) SIGNAL LINE REQUIREMENTS

**A5.1. Signal Line Requirements.** The PDS carrier provides physical security preventing direct access to the signal line. However, wire signal lines are known to emanate the intended signal. Where the PDS is metallic, the intended signal will couple to the PDS carrier providing direct access to the signal. The requirement is to contain any emanations of the intended unencrypted signal within the PDS. Use shielded metallic wire cable, shielded metallic wire lines, or fiber optics in hardened PDS. Shielded metallic are preferred but not required for simple PDS. Meet this mandatory requirement as follows:

***NOTE:*** Do not confuse the requirements to contain emanations of the intended unencrypted signal with Emission Security (EMSEC) countermeasures. Different technical intercept methods are used for the two signal types, EMSEC being more difficult and complex. EMSEC countermeasures are applied to contain unintended compromising emanations within the inspectable space.

A5.1.1. Shielded Wire Lines. Use shielded twisted-pair (STP) or shielded multiconductor wire cable. Each STP or cable must have a minimum of one overall nonferrous shield and must meet the requirements of paragraph **A5.2.** Ground the shield at one end, closest to the equipment, to a facility signal ground. Keep pigtails less than 1 inch (2.5 cm) in length and ground-wire shield terminations as short as possible. Long pigtails and terminations drastically reduce shielding effectiveness and, in certain frequency ranges (dependent on pigtail length), can completely nullify the inherent shielding capability of a cable. Crosstalk is permitted on adjacent pairs within a bundle. Always follow equipment manufacturer's recommendations for cabling provided with equipment.

A5.1.2. Shielded Coaxial Cables. Typically, the shield of a coaxial cable (outer conductor) is used as a signal return path connected to a signal ground within the equipment. However, the signal ground within the equipment is not necessarily connected to a facility signal ground. When the equipment is not connected to a facility signal ground, the coaxial cable can radiate low-level emanations of the intended signal. In this case, use shielded coaxial (triaxial) cable. Use a second shield insulated from any metallic carrier portion of the PDS and insulated from the coaxial return path or use triaxial cable. The shielding must meet the requirements of paragraph **A5.2.** Ground the shield at one end, closest to the equipment, to a facility signal ground. Keep pigtails less than 1 inch (2.5 cm) in length and ground-wire shield terminations as short as possible. Long pigtails and terminations drastically reduce shielding effectiveness and, in certain frequency ranges (dependent on pigtail length), can completely nullify the inherent shielding capability of a cable.

A5.1.3. Unshielded Coaxial Cable. Unshielded coaxial cable may be used if the shield is connected to a signal ground within the equipment at both ends of the PDS and, in turn, each equipment's signal ground is connected to a facility signal ground.

A5.1.4. Fiber Optic Cables. Use opaque-clad fiber optic cable. It is not necessary to shield fiber optic cables. A fiber optic cable should not contain a metallic conductor of any type (strength members, armor, or metallic particles in the coloring of the cladding). Such metallic conductors can become fortuitous conductors for compromising emanations. If such cables are used, treat them in the same manner as the shield on shielded wire lines; that is, the metallic component must be grounded at one end, closest to the equipment, within the CAAs to a facility signal ground.

**A5.2. Shielded Cable Requirements.**

A5.2.1. Physical Cable Characteristics. There are two ways to shield a cable:

A5.2.1.1. Tinned Copper Braid. The cable has an overall shielding of 85 to 90 percent tinned copper-braid coverage. A drain wire is not required in braided-copper shielded cable.

A5.2.1.2. Foil Wrapped. This form of shielded cable can only be used for voice signals and digital signals below 5,000 bits per second. The foil wraps the cable in an overlapping spiral. The overlaps must be z-locked.

A5.2.2. Electrical Cable Characteristics. Shielding must meet the following requirements:

A5.2.2.1. 100 decibels (dB) from 300 to 15,000 hertz.

A5.2.2.2. 80 dB over the baseband video range up to 5 megahertz (MHz).

A5.2.2.3. 60 dB over the frequency range from one to ten times the basic data rate of the digital signal.

## Attachment 6

## PROTECTED DISTRIBUTION SYSTEMS (PDS) CONSTRUCTION REQUIREMENTS

**A6.1. General.** This attachment provides requirements for designing and constructing a PDS to provide the required physical security of the signal line. It does not provide the requirements for safety standards, local building codes, electrical codes, and grounding requirements. This attachment does not preclude the user to purchase commercial hardened PDS.

**A6.2. Design and Construction Objective.** The intent of these requirements in combination with operational security procedures is to allow for rapid detection of any attempted penetration of the carrier rather than ensuring the prevention of a penetration.

***NOTE:*** Take precautions to ensure that general construction practices do not void the security requirements of other paragraphs in this manual.

**A6.3. Design Requirements.**

A6.3.1. Make diagrams showing the proposed route and all involved CAAs, LCAs, and UAAs.

A6.3.2. Make diagrams identifying other wiring, lines, and electrical equipment located along the proposed route within 1 meter of the proposed PDS.

A6.3.3. Include a listing of materials proposed for use to construct the PDS or provide a list of the commercial PDS components, including vendor's name.

**A6.4. Hardened Distribution System.** This distribution system must provide significant physical security protection for the signal line and is implemented by either the hardened carrier, alarmed carrier, or the continuously viewed carrier as follows:

A6.4.1. Hardened Carrier. The principal protection concept for a hardened carrier is to provide for unencumbered visual inspections to detect penetration, tampering, or unauthorized access to the signal line within the carrier.

A6.4.1.1. Do not conceal the carrier from view by placing it behind walls, above ceilings, or below floors, unless the PDS is alarmed or buried. This requirement is to ensure the detection of any penetration of the carrier and preclude hampering that detection.

A6.4.1.2. Provide at least 2.5 centimeters (1 inch) of clearance from walls; floors; ceilings; other wires, cables, ducts; and material that may obstruct viewing during visual inspections. If a wall, floor, or ceiling is at least 20 centimeters (8 inches) of reinforced concrete, you may secure the carrier flush to the wall, floor, or ceiling instead of leaving a 2.5-centimeter gap. Flush mounting cannot leave gaps more than 5 millimeters or slack where the carrier could be temporarily pulled away from the surface providing access to the part hidden from view (against the surface). Secure the carrier to the surface at least once every meter for electrical metallic tubing (EMT) or 2 meters for ferrous conduit or pipe or rigid metallic square tube pipe or rigid sheet steel ducting. **Flexible conduit is not allowed**. The method for securing the carrier to the surface must either prevent removing and reinstalling a support bracket or clip, or allow the lines route inspector to detect if a bracket or clip has been removed and reinstalled.

A6.4.1.3. If the carrier penetrates a wall, ceiling, or floor:

A6.4.1.3.1. If the carrier is firmly anchored so it cannot be moved back and forth, minimum clearance is acceptable. The method for anchoring the carrier must either prevent removing and reinstalling a support bracket or clip, or must allow the lines route inspector to detect if a bracket or clip has been removed and reinstalled. The carrier may also be permanently anchored by using concrete, cement, or a suitable substance to secure the carrier. In this penetration area, any open space around the PDS may be filled with permanent filler, sealant, concrete, or foam.

A6.4.1.3.2. If the carrier cannot be anchored and can be moved back and forth, provide at least 2.5 centimeters of clearance all the way around the carrier (minimum 10-centimeter hole) for thickness up to 10 centimeters. Double the clearance for each additional 10 centimeters (minimum 20-centimeter hole for 10- to 20-centimeter thickness). Center the carrier in the hole.

A6.4.1.3.3. In this penetration area, any open space around the PDS may NOT be filled. A filler (bat insulation for instance) that is easily removed and reinstalled without tools to facilitate lines route inspections may be used.

A6.4.1.4. Within the same level CAA, consider the distribution system and signal line as a RED signal line.

A6.4.1.5. Construct the carrier of EMT with ferrous conduit or pipe, or rigid-sheet steel ducting 16 gauge or better, using elbows, couplings, nipples, and connectors of the same material. Commercially available metallic PDS systems must be approved by DAA or CTTA prior to purchase.

A6.4.1.6. Permanently seal (weld or epoxy) all connections completely around all surfaces. Hinged covers for rigid sheet ducting may be used if the hinges and edges are welded, or use tamper-proof hinges and fasten with tamper-proof hasps and high security padlocks. When securing the hinged covers with padlocks, position tamper-proof hasps close enough together to cause permanent warping of the cover if an attempt is made to gain access by prying up the cover.

A6.4.1.7. High-security padlocks must meet AFI 31-101, *The Air Force Installation Security Program*, specifications or GSA three-position combination padlock FF-P-110 standards, or high-security combination locks that meet the requirements of Federal Specification FF-L-2740A. Another alternative is the General Field Service Padlock (GFSP). The GFSP is the result of a study conducted by the DOD. GFSP provides resistance to forced entry equal to the hardened chain or hasp it will be used with and high resistance to a variety of adverse environmental conditions. Federal specification FF-P-2827, Padlock, General Field Service, was developed for procuring the padlocks. The GFSP is available through the Federal Supply System in two sizes. The national stock number (NSN) for 3/8-inch diameter shackle padlocks is 5340-01-380-9430. The NSN for 1/2-inch diameter shackle padlocks is 5340-01-380-9432.

A6.4.1.8. If pull boxes are used, construct them of metal welded permanently and completely around all surfaces, 16 gauge or better. For Outside the U.S., Medium Threat areas, use 12 gauge or better for pull boxes. Either completely seal (weld or epoxy) the pull box covers around the mating surfaces after construction or use tamper-proof hinges and hasps, and secure the pull boxes with a high security padlock. Do not use boxes with prepunched knockouts.

A6.4.1.9. Do not paint or cover the carrier with wallpaper or any other covering. Such covering can conceal surreptitious penetration of the carrier. Paint and coverings are easier to match than the bare metal when attempting to hide unauthorized penetration.

A6.4.1.10. If a lockbox is required, extend the carrier to it using the same construction requirements as the rest of the carrier. Construct the lockbox of metal, welded permanently and completely around all surfaces, 16 gauge or better, with tamper-proof hinges and tamper-proof hasp. Permanently mount the box to the facility structure at a location convenient to the terminal and to where the carrier terminates within the CAA. Secure the box cover with a high security padlock. Lockboxes can be mounted flush on a wall as long as they can be opened and be inspected. Boxes that are welded shut need to be treated the same as conduit. For Outside the U.S., Medium Threat areas, use 12 gauge or better for pull boxes.

A6.4.2. Buried Carrier. Buried carriers, must be buried a minimum of 1 meter below the surface and on property owned or leased by the U.S. Government or by the contractor having control of the PDS. Secure manholes with a high-security padlock. If specification locks cannot be used, then use a standard locking manhole cover and approved microswitch alarms. Buried carriers outside the U.S. must be encased in approximately 20 centimeters of concrete. If the buried distribution carrier is used for other unclassified signal lines, it must meet the construction requirements for a PDS. Mixing classified and unclassified signal lines within the same carrier is prohibited. One or more separate carriers must be provided for the unclassified signal lines. Within manholes, the PDS carrier must either be extended through the manhole or the ends of the carrier and the RED signal lines must be clearly marked and separated from unclassified signal lines. An inspection of the PDS within the manhole is required each time cleared personnel with the necessary access enter the manhole.

A6.4.3. Suspended Carrier. Carriers suspended above ground are specifically allowed or permitted on property owned or leased by the U.S. Government or contractor having control of the PDS. Suspend the carriers at least 5 meters above the ground. Provide unimpeded inspection of the installed suspended carrier. The carrier must be clear of any obstruction or device that would encroach upon the carrier to facilitate tampering.

A6.4.3.1. Illuminate the carrier.

A6.4.4. Alarmed Carrier. See paragraph **A6.6.** for specific alarm system requirements.

A6.4.4.1. Alarmed carriers may be hidden from view.

A6.4.4.2. Construction of the alarmed carrier is identical to a hardened carrier.

A6.4.4.3. Above ground carriers may be alarmed.

A6.4.5. Continuously Viewed Carrier. Use of a continuously viewed carrier requires constant surveillance, 24 hours-a-day, 7 days-a-week, not just when operational. Circuits may be grouped together if separate from all noncontinuously viewed circuits to ensure an open field of view.

A6.4.5.1. Do not conceal the carrier from view by placing it behind walls, above ceilings, or below floors.

A6.4.5.2. Standing orders include the requirement to investigate any attempt to disturb the carrier.

A6.4.5.3. Immediately contact appropriate security personnel.

A6.4.5.4. This type of carrier cannot be used for TOP SECRET or SPECAT information in any areas outside the U.S.; within the U.S., it cannot be used on property leased by the U.S. Government or contractor-controlled property.

A6.4.5.5. If a lockbox is required, follow the same requirements of paragraph **A6.4.1.10.**.

**A6.5. Simple Distribution System.** This system provides a reduced level of physical protection as compared to the hardened distribution system. When allowed by **Table A4.1.** and **Table A4.2.**, construct the simple distribution system as follows:

A6.5.1. The Simple Distribution System carrier may be installed behind walls, above ceilings, or below floors, in areas with true floor-to-ceiling walls, as long as it conforms to the requirements of **Table A4.1.** and **Table A4.2.**.

A6.5.2. Within the same level CAA, consider the distribution system and signal line as a RED signal line, not as a PDS.

A6.5.3. Construct the simple PDS carrier of any material (e.g., conduit, EMT, metallic cable tray, etc.). Outside a building within the LCA, construct the carrier of metallic conduit or EMT. Contain access points within the CAA.

A6.5.3.1. If pull boxes are used, seal them to same extent as main carrier.

A6.5.3.2. Do not paint or cover the carrier with wallpaper or any other covering. Such covering can conceal surreptitious penetration of the carrier. Paint and coverings are easier to match than the bare material when attempting to hide unauthorized penetration.

A6.5.3.3. If a lockbox is required, extend the carrier to it using the same construction requirements as the rest of the carrier. Permanently mount the box to the facility structure at a location convenient to the terminal and to where the carrier terminates within the CAA. Secure the box cover to the same level as the main PDS.

A6.5.4. If you suspend the carrier above ground, elevate the carrier a minimum of 5 meters. Make sure the carrier is clear of any obstruction or device that would encroach upon the carrier to facilitate tampering.

**A6.6. Alarm Systems.**

A6.6.1. The alarmed carrier provides automatic detection of attempts to penetrate, tamper, or access the signal line within the carrier.

A6.6.2. There are two alarming methods:

A6.6.2.1. Area Alarm. Apply intrusion detection alarms to the area through which the carrier passes making the area, in effect, a controlled area. Use intrusion detection alarms approved by the cognizant security authority and also meet the criteria in AFI 31-101 for a controlled area at the classification level of the information processed.

A6.6.2.2. Carrier Alarm. Use alarms listed on the Approved Alarm Systems for Protected Distribution Systems. This listing is available at **https://private.afca.af.mil/ip**. Operational plans and procedures for a carrier alarm will be the same as if the carrier were an alarmed controlled area. Carrier alarms must meet the following requirements:

A6.6.2.2.1. When the alarm system fails, it must transmit a line fault message to the annunciator panel.

A6.6.2.2.2. Must provide protection from tampering.

A6.6.2.2.3. Must be capable of prompt detection of any attack on the area it is designed to protect.

A6.6.2.2.4. Must have an annunciator panel in an office manned 24 hours-a-day, 7 days-a-week. The office must be capable of notifying responding forces. Appropriate security personnel respond to the area of attempted penetration within 15 minutes. Contact personnel in charge of space to investigate the PDS.

A6.6.2.2.5. Must be able to register malfunctions.

A6.6.2.2.6. Must have a line fault indicator if the alarm system fails.

A6.6.2.2.7. An alarm condition must shut down the RED signal line within the alarmed area or the alarmed carrier.

A6.6.3. Include all pertinent alarm information in the PDS plan. After an alarm is activated, the signal line cannot be used until an inspection is conducted and the reason for the alarm is determined.

## Attachment 7

## PROTECTED DISTRIBUTION SYSTEMS (PDS) CIRCUIT SEPARATION REQUIREMENTS

**A7.1. Circuit Separation Security Criterion.** Ensure personnel accessing any circuit within the distribution system have an appropriate security clearance. Inhibit inappropriate cross connection of circuits.

**A7.2. Access Controls for Collateral Circuits.**

A7.2.1. Circuits of more than one security classification level may use components of a single distribution system.

A7.2.2. Where the sharing of a single distribution system is feasible, the following criterions are mandatory:

A7.2.2.1. Access Points. Access to all points with breakouts of the higher level circuits must be restricted to appropriately cleared personnel. Access points containing classified circuits of different classification levels that do not have breakouts of the higher level circuits can be serviced by lower level cleared personnel when escorted by appropriately cleared personnel.

A7.2.2.2. Termination Boxes. Locate all termination boxes within the CAA.

**A7.3. Access Controls for Special Category (SPECAT).** The Special Security Office provides the requirements pertaining to access controls for SPECAT.

## Attachment 8

## PROTECTED DISTRIBUTION SYSTEMS (PDS) TECHNICAL INSPECTIONS

**A8.1. General.** This attachment provides requirements for establishing and completing technical inspection of an installed PDS. Conduct technical inspections at the minimum intervals according to **Table A4.4.**. Technical inspections must be performed within the intervals specified, but the schedule should remain random and unannounced. The intervals specified in **Table A4.4.**. are minimum requirements. Sometimes the local threat assessment and risk analysis results may indicate a need for more frequent inspections. In these situations, the DAA should increase the frequency as deemed appropriate.

**A8.2. Responsibilities.** The activity identified in the PDS plan (normally the owning or using activity) ensures completion of inspections according to the schedule. The identified organization will either complete the inspections or coordinate with other organizations on base (e.g., wing communications organization) to have appropriately cleared personnel complete the inspection.

A8.2.1. Because of the technical nature of PDS technical inspections, personnel familiar with communications systems installations and maintenance, or similar technical experience and knowledge of electronics, should conduct or assist in conducting the technical inspections.

**A8.3. Requirements.** Required inspections consist of a detailed visual inspection of the entire PDS route and an electrical characterization of the PDS.

A8.3.1. The detailed visual inspections should include all components such as terminal boxes, junction boxes, pull boxes, associated box covers and cover gaskets, manhole access points, connections, connectors, amplifiers, line conditioning equipment, distribution frame connections, optical transmitters, optical receivers, ground connections, locks, lock hasps, hinges, and lock mechanisms.

A8.3.1.1. Open and inspect every manhole cover, locked terminal box, and other locations where locks are used to secure access points. Change all lock combinations as part of the inspection. Record and store lock combinations according to established directives. Report instances of inoperative locks as a physical security COMSEC incident according to AFI 33-212, (will become AFI 33-201, Volume 3 [FOUO]), and the established reporting procedures.

A8.3.1.2. Accomplish an initial technical inspection at the completion of the PDS installation. Personnel of the installing activity, assisted by personnel from the activity identified to perform the continuing inspections, should accomplish this. During the initial inspection, take photographs of the PDS to document the physical configuration. Pay particular attention to any terminal boxes, junction boxes, pull boxes, manhole access points, and any other areas where access to the PDS cables or wiring may be possible. Ensure each photograph is marked as to the exact position or location of the area photographed. You may devise any system of labeling which will provide for the positive identification of the location shown in the photograph. Narratives that further describe the area shown should also accompany these photographs.

A8.3.1.3. Place the photographs and accompanying narratives in the completed PDS file for use during subsequent inspections to assist in identification of possible tampering. A compilation of photographs, when identified with a specific PDS or system and location may be classified. In all cases, handle, mark, and store this information in accordance with the appropriate security classification level.

A8.3.1.4. During the subsequent technical inspections look for changes in the technical aspects of the PDS (e.g., by-pass circuitry, attachment or removal of devices or components, inappropriate or suspicious signal levels, and mechanical integrity of the PDS).

A8.3.2. The electrical characterization consists of such things as time domain reflectometry (TDR) on wire lines and optical time domain reflectometry on fiber optic signal lines. Measure and record the electrical characteristics of the PDS lines to obtain a baseline electrical profile of the PDS. Accomplish the electrical characterization immediately upon completion of the PDS installation. Such measurements may consist of signal levels, voltage levels, TDR recorded readings, and any other electrical measurements that may be recorded and retained. Use a characterization method that will allow use of locally available test equipment and is within the capabilities of the local operating and maintaining function for conducting subsequent technical inspections. Record and compare measurements taken at subsequent technical inspections to the previously recorded baseline measurements to aid in identifying possible tampering attempts. This information is analyzed and used to determine tampering with the signal lines to ensure the physical security of the PDS.

**Attachment 9**

**INTERIM CHANGE (IC) 2005-1 TO AFMAN 33-221, COMMUNICATIONS SECURITY: PROTECTED DISTRIBUTION SYSTEMS (PDS)**

**26 APRIL 2005**

AIR FORCE INSTRUCTION 33-201, VOLUME 8

OPR: HQ AFCA/EVPI (Mr. Gene Zuratynsky)

Certified by: HQ USAF/XICI (Lt Col Gary W. Klabunde)

Supersedes AFMAN 33-221, 12 April 2004

Pages: 16

Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*) and National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003, *Protected Distribution Systems (PDS)*. It prescribes the construction and approval requirements for a protected distribution system (PDS). This instruction applies to all Air Force military, civilian, and contractor personnel under contract by Department of Defense (DOD), who install and maintain Communications Security: Protected Distribution Systems (PDS). This instruction applies to the Air National Guard. The term major command (MAJCOM), when used in this instruction, includes field operating agencies and direct reporting units. The use of extracts from this instruction is encouraged. Additional instructions and manuals are listed on the Air Force Publishing web site at: **http://www.e-publishing.af.mil** under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this publication, through appropriate command channels, to Headquarters, Air Force Communications Agency, (HQ AFCA/EVPI), 203 W. Losey Street, Room 2200, Scott AFB IL 62225-5222. Refer recommended changes and conflicts between this and other publications to HQ AFCA/EASD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF IMT 847, **Recommendation For Change of Publication**. Send an information copy to HQ United States Air Force (HQ USAF/ XICI), 1800 Air Force Pentagon, Washington DC 20330-1800. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records* (will become AFMAN 33-363), and disposed of in accordance with Web-RIMS *Records Disposition Schedule (RDS)* located at: **https://webrims.amc.af.mil/rds/index.cfm**. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See **Attachment 1** for a glossary of references and supporting information.

***SUMMARY OF REVISIONS***

This change incorporates interim change (IC) 2005-1 (**Attachment 9**). It changes AFMAN 33-221 to AFI 33-201, Volume 8, to comply with Air Staff's direction to align all COMSEC publications under the AFI 33-201 umbrella. It updates office symbols, web addresses, and publications throughout the entire document. A bar ( | ) indicates a revision from the previous edition.

**1. Introduction**. AFI 33-201, (FOUO) *Communications Security (COMSEC)*, (will become AFI 33-201, Volume 1 [FOUO]), requires the use of National Security Agency (NSA)-endorsed communications security (COMSEC) products and services to secure classified telecommunications by all Air Force activities and their contractors. Information systems or networks that process classified national security information in more than one controlled-access area (CAA) and require the transfer of that information between CAAs, must use a secure means of transference-secure telecommunications or courier. If secure telecommunications is chosen, include a secure telecommunications requirement (COMSEC) in the systems security policy. In order of preference, the COMSEC requirement is met by NSA-endorsed COMSEC systems (encryption), NSA-endorsed intrusion detection optical communications system (IDOCS), or a PDS. AFI 33-201 (FOUO) (will become AFI 33-201, Volume 1 [FOUO]), also requires the use of NSA-endorsed COMSEC products, techniques, and protected services to protect certain unclassified, sensitive telecommunications involving Air Force activities and their contractors. When certain unclassified, sensitive information must be protected, and a PDS is chosen, follow the standards in this instruction for CONFIDENTIAL information. **Attachment 2** is a flow chart of the process to design, construct, approve, and operate a PDS.

1.1. Although it is less desirable than encryption, a PDS may be used to transmit unencrypted, clear-text, classified national security information. The PDS must provide adequate electrical, electromagnetic, physical, and procedural safeguards identified in this instruction. In establishing the standards for PDS construction and use, national managers incorporated the philosophy of risk management rather than risk avoidance. As such, the standards specified in this manual are the minimum protection standards based on national guidance. The assumption of any additional risk to lessen the minimum specified standards is not an option. Organizations wishing to discuss this policy may send their specific concerns through command channels to HQ AFCA/EVPI. Develop the technical solution using the process described in AFI 33-103, *Requirements Development and Processing*, to justify a PDS. Using any PDS not meeting the standards of this instruction is prohibited.

3.5. Signal wires in PDS. Do not run BLACK signal wire lines in a PDS with RED signal wire lines because of crosstalk. BLACK fiber optic signal lines may be run in a PDS with RED signal lines, but is discouraged for three reasons. It is difficult to identify BLACK signal lines anywhere within the PDS except at the ends. Any person with a need to access the BLACK signal lines must have the appropriate clearance or be escorted. All breakouts of BLACK signal lines must be made in a CAA. See AFMAN 33-214, Volume 2, *Emission Security Countermeasures Review* (will become AFI 33-203, Volume 3).

9.3. Approving Authorities. Except as noted below, the DAA approves the PDS as a part of the SSAA process for the network or information system the PDS is supporting. AFPD 33-2 requires that all systems be certified and accredited prior to operation. AFI 33-202, *Networks and Computer Security*, (will become AFI 33-202, Volume 4, *Certification and Accreditation),* details the process used to certify and accredit Air Force systems. Complete the requirements of AFI 33-202, (will become AFI 33-202, Volume 4), before obtaining approval to operate.

12.2. Records. Maintain and dispose of program records created by this publication accordance to Air Force Web-RIMS (RDS), Table 33-22 and Rule 13, located at: **https://webrims.amc.af.mil/rds/index.cfm**.

**Attachment 1**

**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION**

***References***

DOD 5200.1-R, *Information Security Program*, January 1997

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFI 31-101, (FOUO) *The Air Force Installation Security Program*

AFI 33-103, *Requirements Development and Processing*

AFI 33-201, (FOUO) *Communications Security (COMSEC)* (will become AFI 33-201, Volume 1 [FOUO])

AFI 33-202, *Network and Computer Security* (will become AFI 33-202, Volume 4, *Certification and Accreditation)*

AFI 33-212, *Reporting COMSEC Deviations* (will become AFI 33-201, Volume 3 [FOUO])

AFMAN 33-214, Volume 1, (S) *Emission Security Assessments* (U) (will become AFI 33-203, Volume 2 [S])

AFMAN 33-214, Volume 2, *Emission Security Countermeasures Reviews* (will become AFI 33-203, Volume 3)

AFMAN 37-123, *Management of Records* (will become AFMAN 33-363)

AFDIR 33-303, *Compendium of Communications and Information Terminology*

NSTISSI No. 7003, *Protected Distribution Systems (PDS)*

Web-RIMS, *Records Disposition Schedule (RDS)*

***Abbreviations and Acronyms***

**AFCA—**Air Force Communications Agency

**AFDIR—**Air Force Directory

**AFI—**Air Force Instruction

**AFMAN—**Air Force Office of Special Investigation

**AFPD—**Air Force Policy Directive

**C&A—**Certification and Accreditation

**CAA—**Controlled Access Area

**COMSEC—**Communications Security

**CSO—**Communications and Information Systems Officer

**CTTA—**Certified TEMPEST Technical Authority

**DAA—**Designated Approving Authority

**dB—**Decibels

**DOD—**Department of Defense

**EMSEC—**Emission Security

**EMT—**Electrical Metallic Tubing

**FOUO—**For Official Use Only

**GFSP—**General Field Service Padlock

**GSA—**General Services Administration

**IA—**Information Assurance

**IDOCS—**Intrusion Detection Optical Communications System

**LCA—**Limited Controlled Area

**MAJCOM—**Major Command

**MHz—**Megahertz

**NSA—**National Security Agency

**NSN—**National Stock Number

**NSTISSI—**National Security Telecommunications and Information Systems Security Instruction

**PDS—**Protected Distribution System

**SIPRNET—**Secret Internet Protocol Router Network

**SSAA—**System Security Authorization Agreement

**SPECAT—**Special Category

**STEM—**Systems Telecommunications Engineering Manager

**STP—**Shielded Twisted-Pair

**TDR—**Time Domain Reflectometry

**UAA—**Uncontrolled Access Area

**USAF—**United States Air Force

**WWW—**World Wide Web

***Terms***

**Access Control** Process of limiting access to the resources of an information system only to authorized users, programs, processes, or other systems.

**Controlled-Access Area (CAA)** The room, building, or facility area under direct physical control within which unauthorized persons are denied unrestricted access and are either escorted by authorized persons or are under continuous physical or electronic surveillance. Within the greater CAA, there are three levels of data control: TOP SECRET/SPECAT, SECRET, and CONFIDENTIAL. Examples of these are open storage areas, secured facilities, and open offices that are locked at night and on weekends. These levels correspond to division of **Table A4.1.** and **Table A4.2.**

**Limited-Control Area (LCA)** The space surrounding a protected distribution system within which exploitation is not considered likely or legal authority to identify or remove a potential exploitation exists. Also known as Inspectable Space.

**Line Route** The actual path of the PDS, including the conductor, inside the PDS.

**Lockbox** A metallic box with a lock attached to the end of the PDS within the CAA large enough to hold the signal line. The purpose of the lockbox is to provide authorized access to classified information when,

and only when, required. Normally, the lockbox houses a live Secret Internet Protocol Router Network (SIPRNET) connection point and therefore is a security container. The lockbox can use an approved padlock or the newer lockbox can use a high security combination lock or electronic lock, similar to the lock on a safe. Lockboxes should be General Service Administration (GSA) approved containers; are covered under DoD 5200.1-R, *Information Security Program*, January 1997; and require a SF 702. See paragraph **A6.4.1.7.** for more information.

**Protected Distribution System (PDS)** A wire line or fiber optics distribution system with adequate electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified national security information. ***NOTE***: This definition does not include IDOCS approved by the NSA.

**Special Category (SPECAT)** The definition is classified (see AFMAN 33-214, Volume 1 [S] *Emission Security Assessment* [U], (will become AFI 33-203, Volume 2 [S]).

**Uncontrolled Access Area (UAA)** The area external or internal to a facility over which no personnel access controls can be or are exercised. The area outside the fence surrounding an Air Force Base, and accessible to the general public is an UAA.

**Table A1.1. World Wide Web (WWW) Sources.**

| Referenced | URL | Topic | Organization | Web Page POC |
|---|---|---|---|---|
| **Attachment 1** | **https://private.afca.af.mil/ip/** | Information Assurance web page | HQ AFCA/EVPI | Web Master:<br>**EVPI Webmaster@scott.af.mil** |
| Purpose Statement | **http://www.e-publishing.af.mil** | Air Force Publishing | AFDPO | **e-publishing@pentagon.af.mil** |
| Purpose Statement | **https://webrims.amc.af.mil/rds/index.cfm** | Web-RIMS RDS | AFCA/RIMS | **web.records@scott.af.mil** |

**Attachment 3**

**PROTECTED DISTRIBUTION SYSTEMS (PDS) OPERATION REQUIREMENTS**

**A3.1. Introduction**. This attachment identifies the operation requirements needed to ensure and maintain the security of the PDS. The operation requirements listed in this attachment are the minimum requirements. Document these requirements with an official memorandum, such as a letter of appointment, an operating instruction, or other official means. Ensure that the wing IA office is kept aware of new PDSs or modifications to existing PDSs. Advise the local Staff Judge Advocate when the PDS traverses UAAs.

**A3.2. Controlling Office**. The Controlling Office is the office of primary responsibility for the PDS operation; with the IA office, civil engineer, and the DAA playing major roles. The DAA is the final authority granting approval to operate.

A3.2.1. Establish the operational security procedures for the PDS. Draft procedures are permitted for validation (see paragraph **6.**). Finalize them for certification (see paragraph **8.**).

A3.2.2. Establish the requirement for all personnel in the CAAs to be aware of their responsibility to assist in the close supervision of the visible components of the PDS. They are to report all incidents of suspicious activity immediately.

**A3.3. Security Office**. Identify a PDS security office or person (may be the same as the Controlling Office or the Record Office). Neither the MAJCOM nor the wing IA office will be identified as the Security Office. This office or person will:

A3.3.1. Establish and review the PDS Log at least monthly.

A3.3.2. Receive reports of alarms (if used) and incidents of tampering, penetration, or unauthorized interception, immediately make the initial investigation, and resolve or notify the specified investigating agency such as Security Forces, Air Force Office of Special Investigations (AFOSI), etc.

A3.3.3. Receive reports of suspicious activity in the area of the PDS, immediately make the initial investigation, and resolve or report such activities to security forces for appropriate action.

A3.3.4. Make required notifications.

**A3.4. Record Office**. Specify the office, or person, to establish and maintain a record of events for the PDS (may be the same as the Controlling Office or the Security Office). Neither the MAJCOM nor the wing IA office will be identified as the Record Office. Record in the PDS Log, all PDS events such as alarms, lines route inspections, technical inspections, and other pertinent information.

**A3.5. Reporting Procedures**. Establish the procedures for reporting incidents of tampering, penetration, or unauthorized interception. These incidents will most likely be discovered during lines route inspections and technical inspections. Ensure these incidents are reported immediately. Specify the means for reporting such as secure telephone, in person, etc. Include the requirement to immediately discontinue using the PDS until the approval authority assesses the incident and its security status is determined.

A3.5.1. Immediately report these incidents to the PDS Security Office, or person, for review and initiation of an investigation.

A3.5.2. Immediately report these incidents as a physical security COMSEC incident following the procedures established for physical security incidents in AFI 33-212, *Reporting COMSEC Deviations* (will become AFI 33-201, Volume 3 [FOUO])

**A3.6. Investigating Procedures**. Establish the procedures for investigating reports of tampering, penetration, or unauthorized interception. This should involve the AFOSI since these incidents could be acts of espionage.

**A3.7. Monitoring Alarms**. If the PDS is alarmed, identify who will monitor the alarm indicator.

**A3.8. Responding to Alarms**. If the PDS is alarmed, establish the requirement to respond to an alarm within 15 minutes and identify the individuals responding.

**A3.9. Investigating Alarms**. If the PDS is alarmed, identify who will initially investigate alarms to determine if an attempt at tampering, penetration, or unauthorized interception is suspected. If an attempt is suspected, notify the specified investigating agency; typically, this is the AFOSI.

**A3.10. Inspections**. Specify the office that will be responsible for conducting the required inspections as delineated in **Attachment 4**.

**A3.11. Testing Requirements**. Each alarm system is unique and therefore has unique testing requirements. Refer to the Vendor's operating and testing instructions.

**Attachment 6**

**PROTECTED DISTRIBUTION SYSTEMS (PDS) CONSTRUCTION REQUIREMENTS**

**A6.1. General**. This attachment provides requirements for designing and constructing a PDS to provide the required physical security of the signal line. It does not provide the requirements for safety standards, local building codes, electrical codes, and grounding requirements. This attachment does not preclude the user to purchase commercial hardened PDS.

**A6.2. Design and Construction Objective**. The intent of these requirements in combination with operational security procedures is to allow for rapid detection of any attempted penetration of the carrier rather than ensuring the prevention of a penetration.

***NOTE:*** Take precautions to ensure that general construction practices do not void the security requirements of other paragraphs in this manual.

**A6.3. Design Requirements**.

A6.3.1. Make diagrams showing the proposed route and all involved CAAs, LCAs, and UAAs.

A6.3.2. Make diagrams identifying other wiring, lines, and electrical equipment located along the proposed route within 1 meter of the proposed PDS.

A6.3.3. Include a listing of materials proposed for use to construct the PDS or provide a list of the commercial PDS components, including vendor's name.

**A6.4. Hardened Distribution System**. This distribution system must provide significant physical security protection for the signal line and is implemented by either the hardened carrier, alarmed carrier, or the continuously viewed carrier as follows:

A6.4.1. Hardened Carrier. The principal protection concept for a hardened carrier is to provide for unencumbered visual inspections to detect penetration, tampering, or unauthorized access to the signal line within the carrier.

A6.4.1.1. Do not conceal the carrier from view by placing it behind walls, above ceilings, or below floors, unless the PDS is alarmed or buried. This requirement is to ensure the detection of any penetration of the carrier and preclude hampering that detection.

A6.4.1.2. Provide at least 2.5 centimeters (1 inch) of clearance from walls; floors; ceilings; other wires, cables, ducts; and material that may obstruct viewing during visual inspections. If a wall, floor, or ceiling is at least 20 centimeters (8 inches) of reinforced concrete, you may secure the carrier flush to the wall, floor, or ceiling instead of leaving a 2.5-centimeter gap. Flush mounting cannot leave gaps more than 5 millimeters or slack where the carrier could be temporarily pulled away from the surface providing access to the part hidden from view (against the surface). Secure the carrier to the surface at least once every meter for electrical metallic tubing (EMT) or 2 meters for ferrous conduit or pipe or rigid metallic square tube pipe or rigid sheet steel ducting. **Flexible conduit is not allowed**. The method for securing the carrier to the surface must either prevent removing and reinstalling a support bracket or clip, or allow the lines route inspector to detect if a bracket or clip has been removed and reinstalled.

A6.4.1.3. If the carrier penetrates a wall, ceiling, or floor:

A6.4.1.3.1. If the carrier is firmly anchored so it cannot be moved back and forth, minimum clearance is acceptable. The method for anchoring the carrier must either prevent removing and reinstalling a support bracket or clip, or must allow the lines route inspector to detect if a bracket or clip has been removed and reinstalled. The carrier may also be permanently anchored by using concrete, cement, or a suitable substance to secure the carrier. In this penetration area, any open space around the PDS may be filled with permanent filler, sealant, concrete, or foam.

A6.4.1.3.2. If the carrier cannot be anchored and can be moved back and forth, provide at least 2.5 centimeters of clearance all the way around the carrier (minimum 10-centimeter hole) for thickness up to 10 centimeters. Double the clearance for each additional 10 centimeters (minimum 20-centimeter hole for 10- to 20-centimeter thickness). Center the carrier in the hole.

A6.4.1.3.3. In this penetration area, any open space around the PDS may NOT be filled. A filler (bat insulation for instance) that is easily removed and reinstalled without tools to facilitate lines route inspections may be used.

A6.4.1.4. Within the same level CAA, consider the distribution system and signal line as a RED signal line.

A6.4.1.5. Construct the carrier of EMT with ferrous conduit or pipe, or rigid-sheet steel ducting 16 gauge or better, using elbows, couplings, nipples, and connectors of the same material. Commercially available metallic PDS systems must be approved by DAA or CTTA prior to purchase.

A6.4.1.6. Permanently seal (weld or epoxy) all connections completely around all surfaces. Hinged covers for rigid sheet ducting may be used if the hinges and edges are welded, or use tamper-proof hinges and fasten with tamper-proof hasps and high security padlocks. When securing the hinged covers with padlocks, position tamper-proof hasps close enough together to cause permanent warping of the cover if an attempt is made to gain access by prying up the cover.

A6.4.1.7. High-security padlocks must meet AFI 31-101, *The Air Force Installation Security Program*, specifications or GSA three-position combination padlock FF-P-110 standards, or high-security combination locks that meet the requirements of Federal Specification FF-L-2740A. Another alternative is the General Field Service Padlock (GFSP). The GFSP is the result of a study conducted by the DOD. GFSP provides resistance to forced entry equal to the hardened chain or hasp it will be used with and high resistance to a variety of adverse environmental conditions. Federal specification FF-P-2827, Padlock, General Field Service, was developed for procuring the padlocks. The GFSP is available through the Federal Supply System in two sizes. The national stock number (NSN) for 3/8-inch diameter shackle padlocks is 5340-01-380-9430. The NSN for 1/2-inch diameter shackle padlocks is 5340-01-380-9432.

A6.4.1.8. If pull boxes are used, construct them of metal welded permanently and completely around all surfaces, 16 gauge or better. For Outside the U.S., Medium Threat areas, use 12 gauge or better for pull boxes. Either completely seal (weld or epoxy) the pull box covers around the mating surfaces after construction or use tamper-proof hinges and hasps, and secure the pull boxes with a high security padlock. Do not use boxes with prepunched knockouts.

A6.4.1.9. Do not paint or cover the carrier with wallpaper or any other covering. Such covering can conceal surreptitious penetration of the carrier. Paint and coverings are easier to match than the bare metal when attempting to hide unauthorized penetration.

A6.4.1.10. If a lockbox is required, extend the carrier to it using the same construction requirements as the rest of the carrier. Construct the lockbox of metal, welded permanently and completely around all sur-

faces, 16 gauge or better, with tamper-proof hinges and tamper-proof hasp. Permanently mount the box to the facility structure at a location convenient to the terminal and to where the carrier terminates within the CAA. Secure the box cover with a high security padlock. Lockboxes can be mounted flush on a wall as long as they can be opened and be inspected. Boxes that are welded shut need to be treated the same as conduit. For Outside the U.S., Medium Threat areas, use 12 gauge or better for pull boxes.

A6.4.2. Buried Carrier. Buried carriers, must be buried a minimum of 1 meter below the surface and on property owned or leased by the U.S. Government or by the contractor having control of the PDS. Secure manholes with a high-security padlock. If specification locks cannot be used, then use a standard locking manhole cover and approved microswitch alarms. Buried carriers outside the U.S. must be encased in approximately 20 centimeters of concrete. If the buried distribution carrier is used for other unclassified signal lines, it must meet the construction requirements for a PDS. Mixing classified and unclassified signal lines within the same carrier is prohibited. One or more separate carriers must be provided for the unclassified signal lines. Within manholes, the PDS carrier must either be extended through the manhole or the ends of the carrier and the RED signal lines must be clearly marked and separated from unclassified signal lines. An inspection of the PDS within the manhole is required each time cleared personnel with the necessary access enter the manhole.

A6.4.3. Suspended Carrier. Carriers suspended above ground are specifically allowed or permitted on property owned or leased by the U.S. Government or contractor having control of the PDS. Suspend the carriers at least 5 meters above the ground. Provide unimpeded inspection of the installed suspended carrier. The carrier must be clear of any obstruction or device that would encroach upon the carrier to facilitate tampering.

A6.4.3.1. Illuminate the carrier.

A6.4.4. Alarmed Carrier. See paragraph **A6.6.** for specific alarm system requirements.

A6.4.4.1. Alarmed carriers may be hidden from view.

A6.4.4.2. Construction of the alarmed carrier is identical to a hardened carrier.

A6.4.4.3. Above ground carriers may be alarmed.

A6.4.5. Continuously Viewed Carrier. Use of a continuously viewed carrier requires constant surveillance, 24 hours-a-day, 7 days-a-week, not just when operational. Circuits may be grouped together if separate from all noncontinuously viewed circuits to ensure an open field of view.

A6.4.5.1. Do not conceal the carrier from view by placing it behind walls, above ceilings, or below floors.

A6.4.5.2. Standing orders include the requirement to investigate any attempt to disturb the carrier.

A6.4.5.3. Immediately contact appropriate security personnel.

A6.4.5.4. This type of carrier cannot be used for TOP SECRET or SPECAT information in any areas outside the U.S.; within the U.S., it cannot be used on property leased by the U.S. Government or contractor-controlled property.

A6.4.5.5. If a lockbox is required, follow the same requirements of paragraph **A6.4.1.10.**.

**A6.5. Simple Distribution System**. This system provides a reduced level of physical protection as compared to the hardened distribution system. When allowed by **Table A4.1.** and **Table A4.2.**, construct the simple distribution system as follows:

A6.5.1. The Simple Distribution System carrier may be installed behind walls, above ceilings, or below floors, in areas with true floor-to-ceiling walls, as long as it conforms to the requirements of **Table A4.1.** and **Table A4.2.**.

A6.5.2. Within the same level CAA, consider the distribution system and signal line as a RED signal line, not as a PDS.

A6.5.3. Construct the simple PDS carrier of any material (e.g., conduit, EMT, metallic cable tray, etc.). Outside a building within the LCA, construct the carrier of metallic conduit or EMT. Contain access points within the CAA.

A6.5.3.1. If pull boxes are used, seal them to same extent as main carrier.

A6.5.3.2. Do not paint or cover the carrier with wallpaper or any other covering. Such covering can conceal surreptitious penetration of the carrier. Paint and coverings are easier to match than the bare material when attempting to hide unauthorized penetration.

A6.5.3.3. If a lockbox is required, extend the carrier to it using the same construction requirements as the rest of the carrier. Permanently mount the box to the facility structure at a location convenient to the terminal and to where the carrier terminates within the CAA. Secure the box cover to the same level as the main PDS.

A6.5.4. If you suspend the carrier above ground, elevate the carrier a minimum of 5 meters. Make sure the carrier is clear of any obstruction or device that would encroach upon the carrier to facilitate tampering.

**A6.6. Alarm Systems**.

A6.6.1. The alarmed carrier provides automatic detection of attempts to penetrate, tamper, or access the signal line within the carrier.

A6.6.2. There are two alarming methods:

A6.6.2.1. Area Alarm. Apply intrusion detection alarms to the area through which the carrier passes making the area, in effect, a controlled area. Use intrusion detection alarms approved by the cognizant security authority and also meet the criteria in AFI 31-101 for a controlled area at the classification level of the information processed.

A6.6.2.2. Carrier Alarm. Use alarms listed on the Approved Alarm Systems for Protected Distribution Systems. This listing is available at **https://private.afca.af.mil/ip**. Operational plans and procedures for a carrier alarm will be the same as if the carrier were an alarmed controlled area. Carrier alarms must meet the following requirements:

A6.6.2.2.1. When the alarm system fails, it must transmit a line fault message to the annunciator panel.

A6.6.2.2.2. Must provide protection from tampering.

A6.6.2.2.3. Must be capable of prompt detection of any attack on the area it is designed to protect.

A6.6.2.2.4. Must have an annunciator panel in an office manned 24 hours-a-day, 7 days-a-week. The office must be capable of notifying responding forces. Appropriate security personnel respond to the area of attempted penetration within 15 minutes. Contact personnel in charge of space to investigate the PDS.

A6.6.2.2.5. Must be able to register malfunctions.

A6.6.2.2.6. Must have a line fault indicator if the alarm system fails.

A6.6.2.2.7. An alarm condition must shut down the RED signal line within the alarmed area or the alarmed carrier.

A6.6.3. Include all pertinent alarm information in the PDS plan. After an alarm is activated, the signal line cannot be used until an inspection is conducted and the reason for the alarm is determined.

**Attachment 8**

**PROTECTED DISTRIBUTION SYSTEMS (PDS) TECHNICAL INSPECTIONS**

**A8.1. General**. This attachment provides requirements for establishing and completing technical inspection of an installed PDS. Conduct technical inspections at the minimum intervals according to **Table A4.4.**. Technical inspections must be performed within the intervals specified, but the schedule should remain random and unannounced. The intervals specified in **Table A4.4.**. are minimum requirements. Sometimes the local threat assessment and risk analysis results may indicate a need for more frequent inspections. In these situations, the DAA should increase the frequency as deemed appropriate.

**A8.2. Responsibilities**. The activity identified in the PDS plan (normally the owning or using activity) ensures completion of inspections according to the schedule. The identified organization will either complete the inspections or coordinate with other organizations on base (e.g., wing communications organization) to have appropriately cleared personnel complete the inspection.

A8.2.1. Because of the technical nature of PDS technical inspections, personnel familiar with communications systems installations and maintenance, or similar technical experience and knowledge of electronics, should conduct or assist in conducting the technical inspections.

**A8.3. Requirements**. Required inspections consist of a detailed visual inspection of the entire PDS route and an electrical characterization of the PDS.

A8.3.1. The detailed visual inspections should include all components such as terminal boxes, junction boxes, pull boxes, associated box covers and cover gaskets, manhole access points, connections, connectors, amplifiers, line conditioning equipment, distribution frame connections, optical transmitters, optical receivers, ground connections, locks, lock hasps, hinges, and lock mechanisms.

A8.3.1.1. Open and inspect every manhole cover, locked terminal box, and other locations where locks are used to secure access points. Change all lock combinations as part of the inspection. Record and store lock combinations according to established directives. Report instances of inoperative locks as a physical security COMSEC incident according to AFI 33-212, (will become AFI 33-201, Volume 3 [FOUO]), and the established reporting procedures.

A8.3.1.2. Accomplish an initial technical inspection at the completion of the PDS installation. Personnel of the installing activity, assisted by personnel from the activity identified to perform the continuing inspections, should accomplish this. During the initial inspection, take photographs of the PDS to document the physical configuration. Pay particular attention to any terminal boxes, junction boxes, pull boxes, manhole access points, and any other areas where access to the PDS cables or wiring may be possible. Ensure each photograph is marked as to the exact position or location of the area photographed. You may devise any system of labeling which will provide for the positive identification of the location shown in the photograph. Narratives that further describe the area shown should also accompany these photographs.

A8.3.1.3. Place the photographs and accompanying narratives in the completed PDS file for use during subsequent inspections to assist in identification of possible tampering. A compilation of photographs,

when identified with a specific PDS or system and location may be classified. In all cases, handle, mark, and store this information in accordance with the appropriate security classification level.

A8.3.1.4. During the subsequent technical inspections look for changes in the technical aspects of the PDS (e.g., by-pass circuitry, attachment or removal of devices or components, inappropriate or suspicious signal levels, and mechanical integrity of the PDS).

A8.3.2. The electrical characterization consists of such things as time domain reflectometry (TDR) on wire lines and optical time domain reflectometry on fiber optic signal lines. Measure and record the electrical characteristics of the PDS lines to obtain a baseline electrical profile of the PDS. Accomplish the electrical characterization immediately upon completion of the PDS installation. Such measurements may consist of signal levels, voltage levels, TDR recorded readings, and any other electrical measurements that may be recorded and retained. Use a characterization method that will allow use of locally available test equipment and is within the capabilities of the local operating and maintaining function for conducting subsequent technical inspections. Record and compare measurements taken at subsequent technical inspections to the previously recorded baseline measurements to aid in identifying possible tampering attempts. This information is analyzed and used to determine tampering with the signal lines to ensure the physical security of the PDS.